

May 2010

# INFORMATION SECURITY

## Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>MAY 2010</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2010 to 00-00-2010</b>	
4. TITLE AND SUBTITLE <b>Information Security: Federal Guidance Needed to Address Control Issues With Implementing Cloud Computing</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>United States Government Accountability Office, 441 G St NW, Washington, DC, 20548</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>53</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			



Highlights of [GAO-10-513](#), a report to congressional requesters

## Why GAO Did This Study

Cloud computing, an emerging form of computing where users have access to scalable, on-demand capabilities that are provided through Internet-based technologies, has the potential to provide information technology services more quickly and at a lower cost, but also to introduce information security risks. Accordingly, GAO was asked to (1) identify the models of cloud computing, (2) identify the information security implications of using cloud computing services in the federal government, and (3) assess federal guidance and efforts to address information security when using cloud computing. To do so, GAO reviewed relevant publications, white papers, and other documentation from federal agencies and industry groups; conducted interviews with representatives from these organizations; and surveyed 24 major federal agencies.

## What GAO Recommends

GAO is recommending that the Office of Management and Budget, General Services Administration, and the Department of Commerce take several steps to address cloud computing security, including completion of a strategy, consideration of security in a planned procurement of cloud computing services, and issuance of guidance related to cloud computing security. In comments on a draft of this report, these agencies generally concurred with GAO's recommendations and described efforts under way to implement them.

View [GAO-10-513](#) or [key components](#).  
For more information, contact Gregory C. Wilshusen (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov).

# INFORMATION SECURITY

## Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing

### What GAO Found

Cloud computing has several service and deployment models. The service models include the provision of infrastructure, computing platforms, and software as a service. The deployment models relate to how the cloud service is provided. They include a private cloud, operated solely for an organization; a community cloud, shared by several organizations; and a public cloud, available to any paying customer.

Cloud computing can both increase and decrease the security of information systems in federal agencies. Potential information security benefits include those related to the use of virtualization, such as faster deployment of patches, and from economies of scale, such as potentially reduced costs for disaster recovery. Risks include dependence on the security practices and assurances of a vendor, dependency on the vendor, and concerns related to sharing of computing resources. However, these risks may vary based on the cloud deployment model. Private clouds may have a lower threat exposure than public clouds, but evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation.

Federal agencies have begun efforts to address information security issues for cloud computing, but key guidance is lacking and efforts remain incomplete. Although individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance. For example, only nine agencies reported having approved and documented policies and procedures for writing comprehensive agreements with vendors when using cloud computing. Agencies have also identified challenges in implementing existing federal information security guidance and the need to streamline and automate the process of implementing this guidance. These concerns include having a process to assess vendor compliance with government information security requirements and the division of information security responsibilities between the customer and vendor. Furthermore, while several governmentwide cloud computing security initiatives are under way by organizations such as the Office of Management and Budget (OMB) and the General Services Administration (GSA), little has been completed as a result of these efforts. For example, OMB has not yet finished a cloud computing strategy. GSA has begun a procurement for cloud computing services, but has faced challenges in completing the procurement due in part to information security concerns. In addition, while the Department of Commerce's National Institute of Standards and Technology has begun efforts to address cloud computing information security, it has not yet issued cloud-specific security guidance. Until specific guidance and processes are developed to guide agencies in planning for and establishing information security for cloud computing, they may not have effective information security controls in place for cloud computing programs.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Background	2
	Cloud Computing Is a Form of Shared Computing with Several Service and Deployment Models	10
	Cloud Computing Has Both Positive and Negative Information Security Implications	15
	Federal Agencies Have Begun Efforts to Address Information Security Issues for Cloud Computing, but Specific Guidance Is Lacking and Efforts Remain Incomplete	20
	Conclusions	28
	Recommendations for Executive Action	28
	Agency Comments and Our Evaluation	29
<b>Appendix I</b>	<b>Objectives, Scope, and Methodology</b>	<b>32</b>
<b>Appendix II</b>	<b>Cloud Computing Case Studies</b>	<b>35</b>
<b>Appendix III</b>	<b>Comments from the Office of Management and Budget</b>	<b>41</b>
<b>Appendix IV</b>	<b>Comments from the General Services Administration</b>	<b>43</b>
<b>Appendix V</b>	<b>Comments from the Department of Commerce</b>	<b>46</b>
<b>Appendix VI</b>	<b>GAO Contact and Staff Acknowledgments</b>	<b>48</b>
<b>Tables</b>		
	Table 1: NIST Essential Characteristics of Cloud Computing	13
	Table 2: Potential Benefits of Cloud Computing	16
	Table 3: Potential Risks of Cloud Computing	19

---

## Figures

Figure 1: Cloud Computing Service Models	12
Figure 2: Cloud Computing Deployment Models	13
Figure 3: NIST Essential Characteristics	14
Figure 4: NASA Nebula Container	37

---

## Abbreviations

CARS	Car Allowance Rebate System
CIO	chief information officer
DOD	Department of Defense
DOT	Department of Transportation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSA	General Services Administration
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
RACE	Rapid Access Computing Environment
SAS	Statement on Auditing Standards
SP	Special Publication

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, DC 20548

May 27, 2010

## Congressional Requesters

Cloud computing, an emerging form of delivering computing services, has been highlighted by the current administration as having the potential to provide information technology (IT) services both more quickly and at a lower cost. Although exact definitions vary, cloud computing can, at a high level, be described as a form of computing where users have access to scalable, on-demand IT capabilities that are provided through Internet-based technologies.

Cloud computing has been reported to have several potential benefits over current systems, including faster deployment of computing resources, a decreased need to buy hardware or to build data centers, and more robust collaboration capabilities. However, along with these benefits are the potential risks that any new form of computing services can bring, including information security breaches, infrastructure failure, and loss of data. Several media reports have described security breaches of cloud infrastructure. Furthermore, other reports have identified security as the major concern hindering federal agencies from adopting cloud computing.

Given these concerns, you asked us to (1) identify the models of cloud computing, (2) identify the information security implications of using cloud computing services in the federal government, and (3) assess federal guidance and efforts to address information security when using cloud computing.

To identify the models of cloud computing, we reviewed publications, guidance, and other documentation from the National Institute of Standards and Technology (NIST), industry groups, and private-sector organizations and then conducted interviews with representatives from these organizations to identify commonly expressed characteristics of cloud computing. To identify information security implications of using cloud computing services in the federal government, we obtained and reviewed publications and guidance from the preceding sources and analyzed them to identify positive and negative information security implications of using cloud computing. We also obtained perceptions of security implications from federal agencies by developing, pretesting, and

---

distributing a survey to 24 major federal agencies.<sup>1</sup> To assess federal guidance and efforts to address information security when using cloud computing, we obtained and analyzed federal information security guidance relevant to cloud computing, identified federal agencies that have implemented cloud computing services, and examined relevant agency security practices related to cloud computing for consistency with existing federal guidance. Appendix I contains additional details on the objectives, scope, and methodology of our review.

We conducted this performance audit from September 2009 through May 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

Cloud computing is an emerging form of computing that relies on Internet-based services and resources to provide computing services to customers, while freeing them from the burden and costs of maintaining the underlying infrastructure. Examples of cloud computing include Web-based e-mail applications and common business applications that are accessed online through a browser, instead of through a local computer. The President's budget has identified the adoption of cloud computing in the federal government as a way to more efficiently use the billions of dollars spent annually on IT.<sup>2</sup> As part of the 2011 budget, the administration plans to deploy cloud computing in a series of pilot projects across the government. According to the President's budget, these pilots could potentially lead to significant savings in federal IT spending. However, along with the potential benefits of using cloud computing come

---

<sup>1</sup>The 24 major federal agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

<sup>2</sup>For fiscal year 2011, the administration has proposed about \$79 billion for IT projects.

---

the potential risks and challenges of adopting a new model for delivering IT services.

---

## Federal Systems and Infrastructure Are at Risk from Cyber Threats

We have previously reported that cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing.<sup>3</sup> Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The threat is substantial and increasing for many reasons, including the ease with which intruders can obtain and use hacking tools and technologies.

Our previous reports and those by agency inspectors general describe serious and widespread information security control deficiencies that continue to place federal assets at risk of inadvertent or deliberate misuse, mission-critical information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. Accordingly, we have designated information security as a governmentwide high-risk area since 1997,<sup>4</sup> a designation that remains in force today.<sup>5</sup>

Further, the growing interconnectivity among information systems, the Internet, and other infrastructure presents increasing opportunities for attacks. For example, in 2009, several media reports described incidents that affected cloud service providers such as Amazon and Google. According to these reports, in December 2009, Amazon's Elastic Compute Cloud experienced two attacks on its cloud infrastructure. Google reported that in December 2009, an attack was made on e-mail accounts that it provided, which resulted in the inadvertent release of sensitive information. Adoption of cloud computing will require federal agencies to

---

<sup>3</sup>GAO, *Continued Efforts Are Needed to Protect Information Systems From Evolving Threats*, [GAO-10-230T](#) (Washington D.C.: Nov. 17, 2009) and *Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, [GAO-09-661T](#) (Washington, D.C.: May 5, 2009).

<sup>4</sup>GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997).

<sup>5</sup>GAO, *High-Risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009).



---

implement new protocols and technologies and interconnect diverse networks and systems while mitigating and responding to threats.

---

**Policies, Procedures, and  
Required Controls Have  
Been Established to  
Protect Federal  
Information and  
Information Systems**

Federal laws and guidance specify requirements for protecting federal systems and data. This includes systems used or operated by a contractor or other organization on behalf of a federal agency, which would include cloud computing. Recognizing the importance of securing federal systems and data, Congress enacted the Federal Information Security Management Act of 2002 (FISMA) to strengthen the security of federal information and information systems within federal agencies. FISMA requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, FISMA requires that information security programs include, among other things, the following:

- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices that include testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

FISMA assigns certain responsibilities to the Office of Management and Budget (OMB) and other responsibilities to NIST. FISMA states that the Director of OMB shall oversee agency information security policies and practices, including

- 
- developing and overseeing the implementation of policies, principles, standards, and guidelines on information security;
  - requiring agencies to identify and provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, or destruction of information collected or maintained by or on behalf of an agency, or information or information systems used or operated by an agency, or by a contractor or other organization on behalf of an agency;
  - overseeing agency compliance with FISMA to enforce accountability; and
  - reviewing, at least annually, and approving or disapproving agency information security programs.

Each year, OMB provides instructions to federal agencies regarding FISMA reporting. In this guidance, for example, OMB has stated that agencies are permitted to utilize private sector data services, provided that appropriate security controls are implemented and, more generally, that agencies ensure that their information security programs apply to all organizations that possess or use federal information, including contractors.

Under FISMA, NIST is tasked with developing, for systems other than national security systems, standards and guidelines that must include, at a minimum, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

Specifically, NIST has developed a risk management framework of standards and guidelines for agencies to follow in developing information security programs. Key publications are

- 
- NIST Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.<sup>6</sup>
  - Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*.<sup>7</sup>
  - FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.<sup>8</sup>
  - NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.<sup>9</sup>

NIST SP 800-37 provides agencies with guidance for applying a risk management framework to federal information systems to include security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. This framework includes the preparation of a security assessment report and authorization package.<sup>10</sup>

FIPS 199 provides agencies with criteria to identify and categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.

---

<sup>6</sup>NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37 Revision 1 (Gaithersburg, Md., February 2010).

<sup>7</sup>NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md., February 2004).

<sup>8</sup>NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md., March 2006).

<sup>9</sup>NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 3 (Gaithersburg, Md., August 2009).

<sup>10</sup>NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems*, SP 800-37 Revision 1 was formerly NIST, *Guide for the Certification and Accreditation of Federal Information Systems*, SP 800-37. The assessment and authorization process replaces the process known as certification and accreditation described in the previous version of SP 800-37.

---

FIPS 200 requires a baseline of minimum information security controls for protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. FIPS 200 directs agencies to implement these baseline control recommendations as follows:

- *Access control*: limit information system access to authorized users and to the types of transactions and functions that authorized users are permitted to exercise.
- *Certification, accreditation, and security assessments*: periodically assess security controls, develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities, authorize operation of systems and any associated system connections, and monitor system security controls on an ongoing basis.
- *Risk assessment*: periodically assess the risk to operations, assets, and individuals, resulting from the operation of systems and the associated processing, storage, or transmission of information.

In applying the provisions of FIPS 200, agencies first categorize their information and systems as required by FIPS 199, and then typically select an appropriate set of security controls from NIST SP 800-53 to satisfy their minimum security requirements. This helps to ensure that appropriate security requirements and security controls are applied to all federal information and information systems including cloud computing.

---

## Selected Organizations Have Established Information Security Guidance for Cloud Computing

As stated previously in this report, federal laws, such as FISMA, and guidance such as that issued by NIST, specify requirements for protecting federal systems and data. Other organizations have developed security models and guidance that specifically apply to cloud computing services. These groups include the Cloud Security Alliance and the European Network and Information Security Agency.

The Cloud Security Alliance is a nonprofit organization formed to promote the use of leading practices for providing security assurance when using cloud computing. In December 2009, the alliance issued Security Guidance

---

for Critical Areas of Focus in Cloud Computing, v2.1.<sup>11</sup> The guidance provides recommendations in 13 cloud computing domains:

- *Architectural framework*: provides a conceptual framework focusing on cloud computing.
- *Governance and enterprise risk management*: ability of an organization to govern and measure enterprise risks.
- *Legal and electronic discovery*: potential legal issues including protection requirements for information and computer systems.
- *Compliance and audit*: proving compliance when using cloud computing during an audit.
- *Information life cycle management*: managing data that is placed in the cloud and determining responsibility for data confidentiality, integrity, and availability.
- *Portability and interoperability*: the ability to move data and services from one provider to another or bring it back in-house.
- *Traditional security, business continuity, and disaster recovery*: identifying where cloud computing may assist in lowering security risks, while potentially increasing it in other areas.
- *Data center operations*: common data center characteristics that could be detrimental to ongoing services, and those that are fundamental to long-term stability.
- *Incident response, notification, and remediation*: addresses complexities that cloud computing brings to an incident handling program and forensics for both the provider and customer.
- *Application security*: securing application software that is either running on or being developed in the cloud.
- *Encryption and key management*: identifying proper encryption usage and scalable key management.

---

<sup>11</sup>Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 2.1 (December 2009).

- 
- *Identity and access management*: focuses on issues encountered when extending an organization's identity into the cloud.
  - *Virtualization*: risks associated with items such as multitenancy, or the sharing of computing resources by different organizations.

For each domain, the guidance documents areas of concern for cloud computing.

The European Network and Information Security Agency is an organization established by the European Union that specializes in information security. In November 2009, the agency issued *Cloud Computing: Benefits, Risks, and Recommendations for Information Security*,<sup>12</sup> which provides a set of information requirements and includes questions that a customer can ask a cloud computing service provider in order to evaluate the service provider's information security practices. The requirements address

- *Personnel security*: policies and procedures when hiring IT administrators or others with system access.
- *Supply chain assurance*: defining and detailing services outsourced or subcontracted, inquiring about the measures taken to ensure third-party service levels are met and maintained, and confirmation that security policy and controls are applied to third party providers.
- *Operational security*: ensuring a provider employs appropriate controls to mitigate unauthorized disclosure of information in addition to defined agreements.
- *Identity and access management*: controls that apply to both the cloud providers and the customer, including access control, authorization, frameworks, identity provisioning, management of personal data, key management, encryption, authentication, and credential compromise or theft.
- *Asset management*: ensuring cloud providers maintain an inventory of the assets under their control.

---

<sup>12</sup>The European Network and Information Security Agency, *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (November 2009).

- 
- *Data and services portability*: clarifying the risks related to becoming dependent on one vendor.
  - *Business continuity management*: maintaining a documented method to determine the impact of a disruption and the relevant response and restoration process.
  - *Physical security*: ensuring the vendor provides adequate physical security for the customers' data.
  - *Environmental controls*: policies and procedures to ensure environmental issues such as fires, floods, and power failures do not cause an interruption of service.
  - *Legal requirements*: compliance with regulatory frameworks.

In addition, the agency's Information Assurance Framework<sup>13</sup> states the need for a clear definition and understanding of security-relevant roles and responsibilities between the customer and the provider.

---

## Cloud Computing Is a Form of Shared Computing with Several Service and Deployment Models

According to NIST, cloud computing is a means “for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”<sup>14</sup> This definition has been generally adopted throughout the federal government. Cloud computing is a form of delivering IT services that takes advantage of several broad evolutionary trends in IT, including the use of virtualization;<sup>15</sup> the decreased cost and increased speed of networked communications, such as the Internet; and overall increases in computing power. As such, any definition of cloud computing will be somewhat broad

---

<sup>13</sup>The European Network and Information Security Agency, *Cloud Computing: Information Assurance Framework* (November 2009).

<sup>14</sup>NIST began developing its definition of cloud computing in November 2008, and its most recent version, version 15, was released in October 2009. See NIST, *The NIST Definition of Cloud Computing*, version 15 (Gaithersburg, Md., Oct. 7, 2009).

<sup>15</sup>Virtualization is a technology that allows multiple, software-based virtual machines, with different operating systems, to run in isolation, side-by-side, on the same physical machine. Virtual machines can be stored as files, making it possible to save a virtual machine and move it from one physical server to another. Virtualization is often used as part of cloud computing.

---

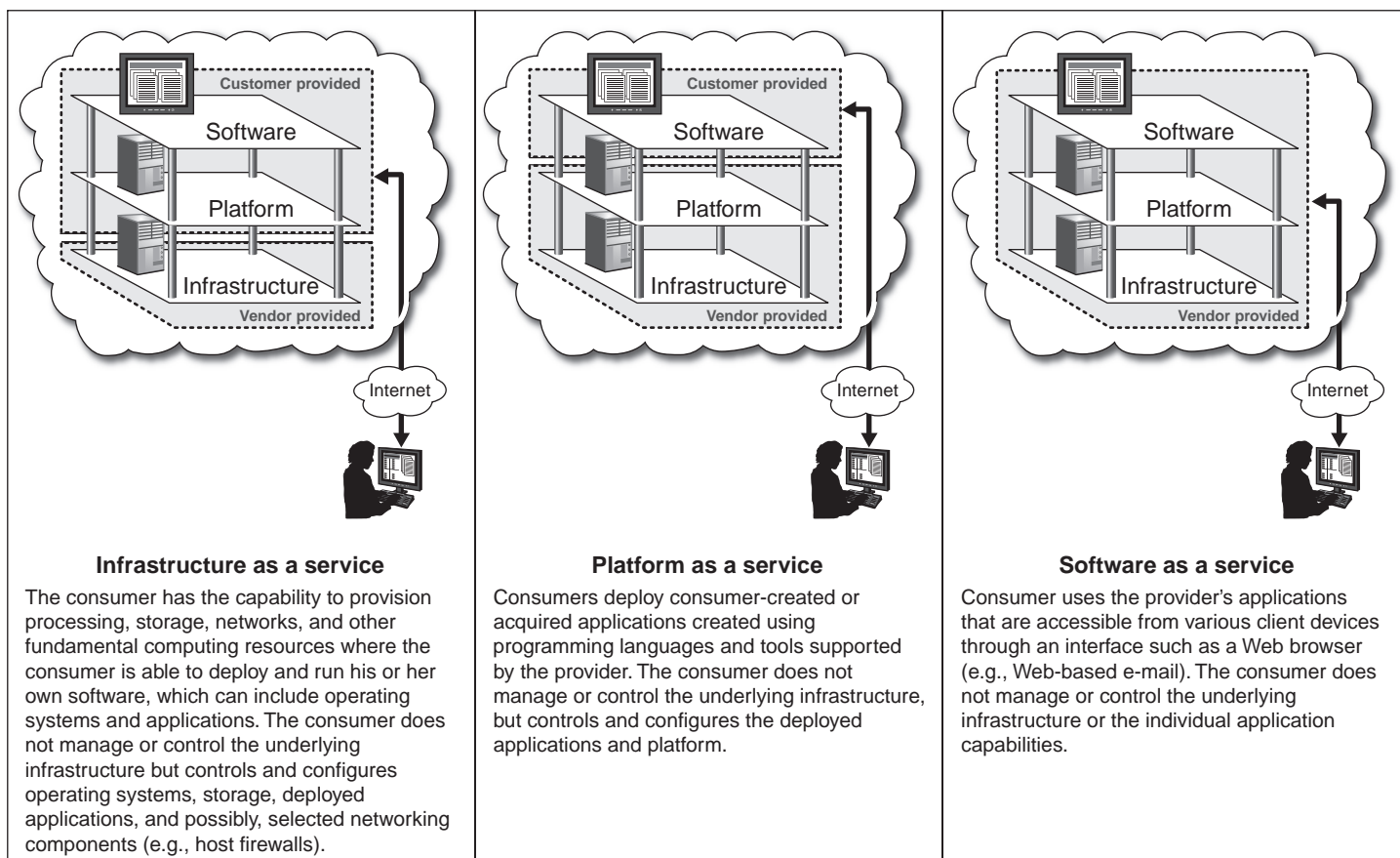
and subject to interpretation. While several other organizations have developed definitions of cloud computing, many of the elements of these definitions are encompassed in the NIST definition.

Cloud computing is further defined by its service and deployment models. There are three service models: infrastructure as a service, platform as a service, and software as a service (see fig.1).

- *Infrastructure as a service* provides various infrastructure components such as hardware, storage, and other fundamental computing resources.
- *Platform as a service* provides a service that runs over an underlying infrastructure. A platform vendor offers a ready-to-use platform, such as an operating system like Microsoft Windows or Linux, which runs on vendor-provided infrastructure. Customers can build applications on a platform using application development frameworks, middleware capabilities, and functions such as databases.
- *Software as a service* runs on an underlying platform and infrastructure managed by the vendor and provides a self-contained operating environment used to deliver a complete application such as Web-based e-mail and related management capabilities.



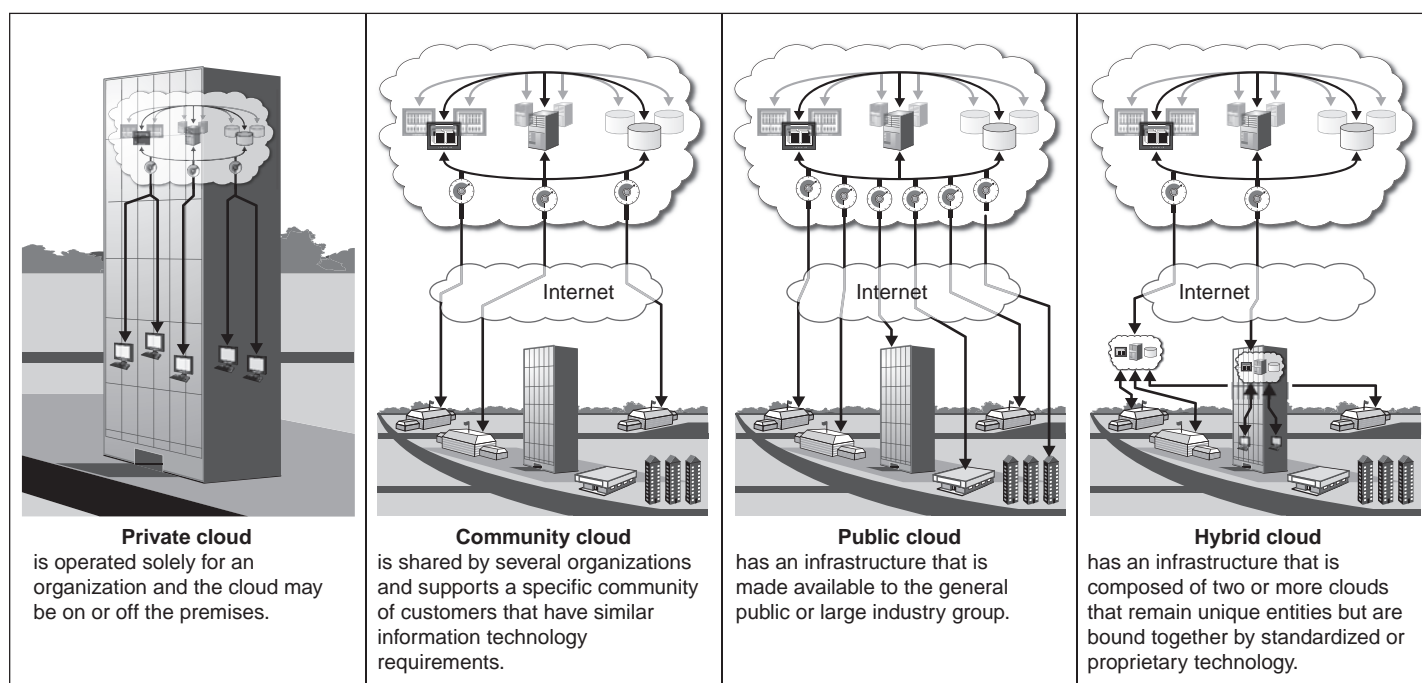
**Figure 1: Cloud Computing Service Models**



Source: GAO analysis of NIST data.

In addition to the service models that describe what can be provided, NIST and other entities describe four deployment models that relate to how the cloud service is provided. These four cloud models are private, community, public, and hybrid (see fig. 2). In a private cloud, the service is set up specifically for one organization, although there may be multiple customers within that organization, and the cloud may exist on or off the premises. In a community cloud, the service is set up for related organizations that have similar requirements. A public cloud is available to any paying customer and is owned and operated by the service provider. A hybrid cloud is a composite of the deployment models.

**Figure 2: Cloud Computing Deployment Models**



Source: GAO analysis of NIST data.

According to NIST, cloud computing includes each of the characteristics listed in table 1 and in figure 3.

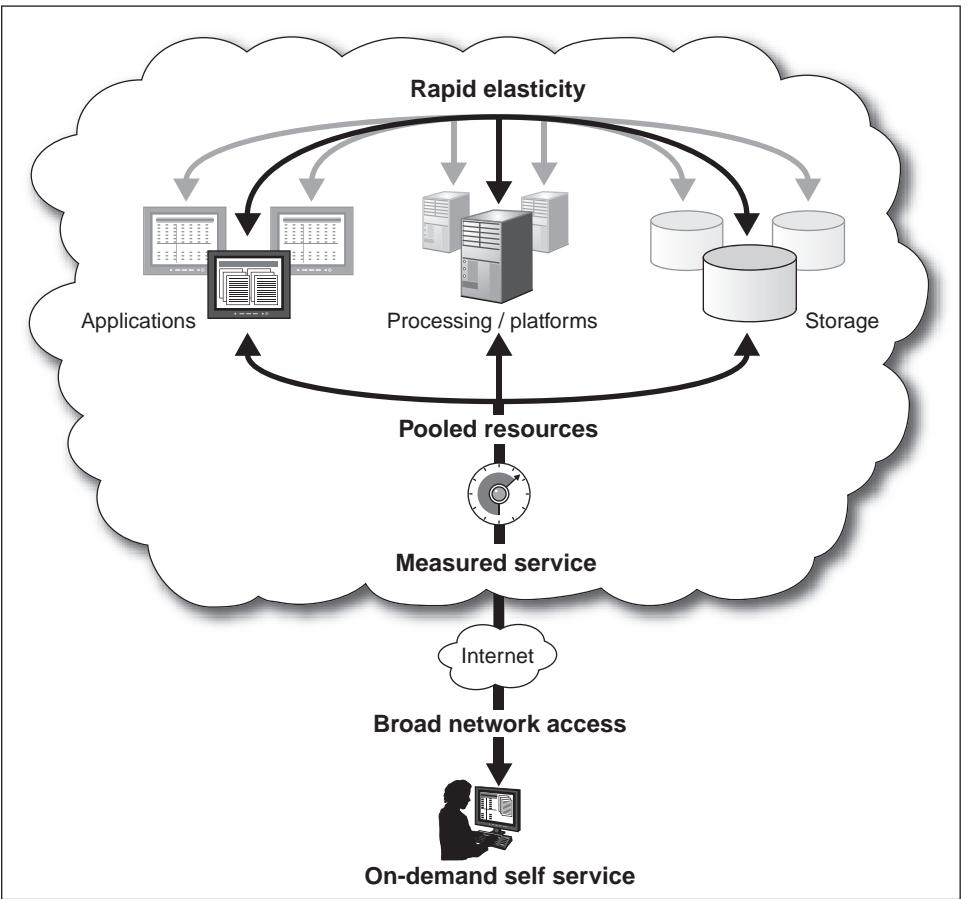
**Table 1: NIST Essential Characteristics of Cloud Computing**

Essential characteristic	Description
On-demand self service	Consumer can unilaterally provision computing capabilities as needed automatically, without interaction with the service's provider.
Broad network access	Capabilities are available over the network and accessed through standard mechanisms such as desktop computers, laptops, mobile phones, and personal digital assistants.
Resource pooling	Provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out (increase) and rapidly released to quickly scale back in (decrease).

Essential characteristic	Description
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering (measured use) capability at some level of abstraction appropriate to the type of service.

Source: GAO analysis of NIST data.

**Figure 3: NIST Essential Characteristics**



Source: GAO.

While NIST states that all five of its essential characteristics should be present for an application to be considered cloud computing, other federal officials and experts stated that an application that has some but not all of these characteristics could still be considered cloud computing.

---

## Cloud Computing Has Both Positive and Negative Information Security Implications

Cloud computing can both increase and decrease the security of information systems. Potential information security benefits include those related to the use of virtualization, such as faster deployment of patches, and from economies of scale, such as potentially reduced costs for disaster recovery. Risks include those related to dependence on the security assurances of a vendor; dependence on the vendor; and concerns related to multitenancy, or sharing computing resources among different organizations. However, these risks may vary based on the cloud deployment model.

---

## Cloud Computing Can Provide Potential Information Security Benefits

The use of cloud computing has the potential to provide several benefits related to information security. These benefits are related to the attributes of cloud computing—specifically, its use of virtualization and automation, broad network access, potential economies of scale, and use of self-service technologies.

The use of virtualization and automation in cloud computing can expedite the implementation of secure configurations for virtual machine images. Department of Defense (DOD) officials responsible for one cloud computing program stated that virtualization allows a cloud computing provider to rapidly replicate secure configurations for cloud-based virtual servers, rather than manually applying secure configurations to physical servers, which could be required in a traditional environment that has not employed virtualization techniques. Private sector representatives also stated that virtualization can allow faster deployment of secure server configurations, security upgrades, and patches for security vulnerabilities than a traditional computing infrastructure can.

Other advantages relate to cloud computing's broad network access and use of Internet-based technologies. For example, several agencies stated that cloud computing provided a reduced need to carry data in removable media because of the ability to access the data through the Internet, regardless of location. NIST officials stated that shifting public data to a public cloud using the Internet that is separate from the agency's internal network is a means of network segmentation that may reduce exposure of sensitive data on the agency's internal network.

Additional advantages relate to the potential economies of scale and distributed nature of cloud computing. For example, in response to our survey, 22 of the 24 agencies identified low-cost disaster recovery and data storage as a potential benefit. Specifically, cloud computing may provide a cheaper way to store backup copies of information. Agencies also stated

that a cloud provider may have more resources to devote to security than the agency may have available. The large-scale and mitigation techniques that cloud providers offer may also reduce vulnerability to denial of service attacks. Department of Transportation (DOT) officials responsible for a cloud computing program noted that the program's Web site, which used a cloud computing service provider, was better able to withstand a denial of service attack because of the use of the cloud provider. The National Aeronautics and Space Administration (NASA) officials responsible for another cloud computing program stated that it may require less effort for cloud computing customers to ensure effective information security if information security controls were already implemented by the provider. Customers could also be freed from the responsibility of maintaining a physical infrastructure, as well as resolving management, operational, and technical issues related to the underlying cloud platform, although the customers would still be responsible for ensuring these issues are addressed and that data are adequately protected.

The self-service aspect of cloud computing may also provide benefits. For example, 20 out of the 24 agencies identified the ability to apply security controls on demand as a potential benefit. A private sector representative stated that cloud computing provided the ability for more flexible and granular control of security. For example, features such as encryption and monitoring could be individually applied as needed. Table 2 lists potential benefits of cloud computing grouped by cloud computing attribute.

**Table 2: Potential Benefits of Cloud Computing**

Attribute	Potential benefit
Virtualization and automation	Rapid replication of securely configured servers, security upgrades, and patches
Broad network access	Reduced need to carry data in removable media Ability to shift data needed by public away from internal agency network
Economies of scale and distributed infrastructure	Low-cost disaster recovery and storage Resistance to denial of service attack
On-demand self-service	Apply security controls on demand Individually apply features such as encryption and monitoring

Source: GAO analysis of agency and private sector data.

---

## Cloud Computing Can Create Information Security Risks

In addition to benefits, the use of cloud computing can create numerous information security risks for federal agencies. Twenty-two of the 24 agencies reported that they are either concerned or very concerned about the potential information security risks associated with cloud computing. These concerns include risks related to being dependent on a vendor's security assurances and the vendor, and risks related to the use of multitenancy.

Several cloud computing information security risks relate to the ability to rely on a vendor's security assurances and practices. Specifically, several agencies stated concerns about

- the possibility of ineffective or noncompliant service provider security controls—which could lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information;
- the potential loss of governance and physical control over agency data and information—that is, in using cloud computing services, the agency cedes control to the provider for the performance of certain security controls and practices;
- the insecure or ineffective deletion of agency data by cloud providers once services have been provided and are complete; and
- potentially inadequate background security investigations for service provider employees—which could lead to an increased risk of wrongful activities by malicious insiders.

Of particular concern is dependency on a vendor. All 24 agencies specifically noted concern about the possibility of loss of data if a cloud computing provider terminated its services. For example, the provider and the customer may not have agreed on terms to transfer or duplicate the data. The European Network and Information Security Agency also identified dependency on a vendor as a high risk, noting the lack of tools, procedures, or standard data formats to ensure data, application, and service portability. The agency stated that this can make it difficult for the customer to migrate from one provider to another or to migrate data and services back to an in-house IT environment. One member of GAO's

---

Executive Council on Information Management and Technology<sup>16</sup> stated that if an agency chooses to implement cloud computing, at some point in the future the vendor may want to raise the cost for use of the cloud. The agency may then have no alternative to paying the cost because it lacks the technical ability to bring the service back in-house.

Multitenancy and use of shared resources can also increase risk. Twenty-three out of the 24 agencies identified multitenancy as a potential information security risk because one customer could intentionally or unintentionally gain access to another customer's data, causing a release of sensitive information.

Additional concerns relate to exchanging authentication information on users and responding to security incidents. For example, NASA officials responsible for a cloud computing program stated that identity management and user authentication are a concern because customers and a provider may need to establish a means to securely exchange and rely on authentication and authorization information for system users. In addition, responding to security incidents may be more difficult in a shared environment because there could be confusion over who performs the specific tasks—the customer or the provider. The Nuclear Regulatory Commission emphasized the importance of a clear delineation of responsibilities as they relate to incident response management, whereby the cloud computing service provider has the responsibility to report the security incident to the agency and the agency is responsible for reporting the incident to the appropriate government entity.

Another concern is the increased volume of data transmitted across agency and public networks. This could lead to an increased risk of the data being intercepted in transit and then disclosed.

NIST also stated that cloud computing security is dependent on the security of a user's Internet browser, and that vulnerabilities in the browser can create vulnerabilities for the cloud computing service.

---

<sup>16</sup>The Executive Council on Information Management and Technology members include experts from the public and private sectors and representatives of related professional organizations who are widely recognized in IT and information management areas. Council members provide expert perspectives to senior GAO executives on performance goals contained in GAO's strategic plan that guide GAO's work in the areas of information security, information management, and IT management.

Although there are numerous potential information security risks related to cloud computing, these risks vary based on the particular deployment model. For example, NIST states that private clouds may have a lower threat exposure than community clouds, which may have a lower threat exposure than public clouds. Officials from another agency stated that they are considering implementing a private cloud behind their agency's firewall because of the moderate-to-high impact classification of sensitive data they were considering placing into this system.<sup>17</sup> Several agency officials and industry representatives stated that initial use of public clouds may be focused on low-impact information. However, several industry representatives also stated that making general statements based on cloud deployment models may be misleading and that an agency would need to examine the specific security controls of the vendor they were evaluating. Table 3 lists potential risks of cloud computing.

**Table 3: Potential Risks of Cloud Computing**

Risk	Explanation
Reliance on vendor's security assurances and practices	An agency is dependent on a provider's ability to ensure effective security. A provider may have security weaknesses such as ineffective or noncompliant security controls. For example, a provider may not maintain adequate physical control over agency data and information or may have inadequate background investigations for provider employees.
Dependence on a vendor	If the agency and provider do not agree on a means to transfer or duplicate data, data may be lost if a provider ends its service. An agency that uses a cloud computing provider may also lose the technical ability to bring the information system back in-house.
Insecure or ineffective identity management	Agencies and a cloud provider may need to securely exchange and rely on sensitive authentication and authorization information for system users.
Unclear responsibilities for incident response	There may be confusion over roles and responsibilities between agency and provider.

Source: GAO analysis of agency and private sector data.

<sup>17</sup>FIPS Special Publication 199 defines three levels of potential impact on organizational operations, assets, or individuals should there be a breach of security. Low applies when the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect; moderate applies when the loss could be expected to have a serious adverse effect on operations, assets, or individuals; and high applies when the loss could be expected to have a severe or catastrophic adverse effect.



---

## Federal Agencies Have Begun Efforts to Address Information Security Issues for Cloud Computing, but Specific Guidance Is Lacking and Efforts Remain Incomplete

Federal agencies have started to address information security when using cloud computing; however, they have not always developed corresponding guidance. Furthermore, agencies that have implemented cloud computing efforts have faced challenges in implementing existing federal information security guidance and identified the need to streamline and automate the process of implementing this guidance. While several governmentwide cloud computing security activities are under way by organizations such as OMB and the General Services Administration (GSA), significant work remains to be completed. In addition, NIST has begun certain efforts related to cloud computing information security, but its existing guidance is not specific to cloud computing issues, and it has only begun plans to issue cloud-specific security guidance.

---

## Agencies Have Taken Steps to Address Information Security Issues for Cloud Computing, but Have Not Always Developed Corresponding Policies or Procedures and Face Challenges in Implementing Existing Guidance and Processes

About half of the 24 agencies we asked reported using some form of cloud computing for obtaining either infrastructure, platform, or software services. These agencies identified measures they are taking or plan to take when using cloud computing. Specifically, 23 of the 24 agencies reported that they currently write or plan to write and enforce comprehensive service-level agreements to include information security control requirements and currently use or plan to use appropriate encryption when using cloud computing. Further, 22 of the 24 agencies responded that they currently limit or plan to limit the type of information placed in a cloud, while 21 of the 24 agencies currently limit or are planning to limit the type of cloud deployment model used. Appendix II includes descriptions of three case studies of cloud computing implementations in the federal government, including steps taken to address information security.

However, these actions have not always been accompanied by the development of related policies or procedures. Of the 23 agencies that reported writing and enforcing or planning to write and enforce comprehensive service-level agreements when using cloud computing, 9 agencies have approved and documented policies and procedures for doing so. Fifteen agencies have documented policies and procedures for the use of encryption. Just four agencies responded that they have documented policies and procedures limiting the type of information placed in a cloud and two agencies responded that they have documented policies and procedures limiting the type of cloud deployment model used. The lack of approved and documented policies and procedures to ensure effective information security when using cloud computing could place sensitive information in a cloud environment at risk.

---

Agencies Have Concerns About Ensuring Vendor Implementation of Information Security Requirements

Most agencies identified challenges and concerns in implementing existing information security laws and guidance. For example, 20 of the 24 agencies identified concerns about service provider compliance with and implementation of government information security requirements. Agencies also expressed concerns about limitations on their ability to conduct independent audits and assessments of security controls of cloud computing service providers.

Several industry representatives agreed that compliance and oversight issues are a concern. However, the representatives also stated that requiring each individual agency that uses a service provider to conduct its own assessment of controls and audits and complete a separate assessment and authorization process would be burdensome and remove the cost advantages offered by cloud computing. In response, representatives raised the idea of having a single government entity or other independent entity conduct security oversight and audits for cloud computing service providers. The process could be similar to the Statement on Auditing Standards (SAS) 70 audit process often used as part of financial audits.<sup>18</sup> A SAS 70 report is issued by an independent auditor for a service provider that processes financial data on behalf of others; it discusses the effectiveness of the service provider's internal controls over the processing of transactions that may be relevant to the financial reporting of customers. Management of the customer organization and its auditor may use this report to assess the internal control policies and procedures at the service provider as part of the overall evaluation of the internal control at the customer organization. Some cloud computing service providers have obtained a SAS 70 audit for use and review by its customers. In discussing the use of SAS 70 reports to meet information security requirements, OMB Memorandum M-09-29<sup>19</sup> states that it is the agency's responsibility to ensure that

- the scope of the SAS 70 audit is sufficient and fully addresses the specific contractor system requiring FISMA review, and

---

<sup>18</sup>SAS 70 will soon be superseded by two new standards: a new audit standard for audits of entities that use service providers and a new attestation standard for reporting on controls at a service provider.

<sup>19</sup>OMB, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Memorandum M-09-29 (Washington, D.C., Aug. 20, 2009).

- 
- the audit encompasses all controls and requirements of law, OMB policy, and NIST guidance.

There are attestation standards, similar to those in SAS 70, that could be used to provide an assessment of controls at a service provider that relates to the effective implementation of security and compliance with specified requirements of laws and guidance. However, the scope of an audit based on a standard such as SAS 70 is defined by the service provider and could exclude key controls essential to effectively protecting agency information. Therefore, if an attestation report on security effectiveness and compliance with laws and guidance is used, it is critical that the scope of the controls addressed by the attestation report is sufficient to meet agency requirements.

Agencies also stated that having a cloud service provider that had been precertified as being in compliance with government information security requirements through some type of governmentwide approval process would make it easier for them to consider using cloud computing. For example, DOT officials implementing the Car Allowance Rebate System program stated that having a cloud service provider that was precertified to process federal financial transactions may have made implementation of the payment processing system for the program easier. Until such precertified providers are in place, the adoption of cloud computing may be limited.

#### Processes, Documentation, and Division of Roles and Responsibilities for Cloud Computing Create Challenges

In their efforts to ensure information security in cloud computing, agencies have had to re-examine and, at times, change related processes, documentation, and roles and responsibilities. For example, DOD officials implementing a cloud computing program identified the need to improve related DOD business processes, including those related to security. The existing DOD process required for risk assessment and assessment and authorization for information systems created challenges because of its focus on stand-alone systems and multiple levels of organizational review. In response, the program office worked with a contractor to re-engineer the process and reduce the time needed to complete information security requirements for new systems. NASA officials also noted the increased complexity of information security-related document maintenance in a shared owner environment and took steps to address this issue.

Other agency concerns related to the division of information security responsibilities between customer and vendor. For example, both DOD and NASA officials responsible for cloud computing implementations at

---

their agencies stated that a clear division of security roles and responsibilities in cloud computing was important. For example, NASA officials divided responsibility for the security controls in NIST SP 800-53 Revision 3 for low-impact systems into customer and provider controls and found that the customer had primary responsibility for 47 of the 112 total controls. Similarly, DOD officials also divided responsibilities for the corresponding DOD information assurance controls between customers and service providers. Both sets of agency officials commented on the challenges in analyzing and maintaining such a division of responsibilities but noted that clear assignment of responsibilities was important for effective information security.

---

**Several Governmentwide Cloud Computing Information Security Initiatives Have Been Started, but Key Guidance and Efforts Have Not Been Completed**

To address cloud computing security issues, the executive branch has begun several initiatives. However, these initiatives have not yet been completed. For example, OMB stated that it began a federal cloud computing initiative in February 2009; however, it does not yet have an overarching strategy or an implementation plan. According to OMB officials, the initiative includes an online cloud computing storefront managed by GSA and will likely contain three pilot cloud computing projects, each with a lead agency: (1) a voucher payment portal led by the Department of the Treasury; (2) a tool for citizen interaction to support open government led by GSA; and (3) a citizen services dashboard led by GSA. However, as of March 2010, a date had not been set for the release of the strategy or for any of the pilots. In addition, OMB has not yet defined how information security issues, such as a shared assessment and authorization process, will be addressed in this strategy.

Federal agencies have stated that additional guidance on cloud computing security would be helpful. Addressing information security issues as part of this strategy would provide additional direction to agencies looking to use cloud computing services. Until this strategy has been completed, agencies will lack clear direction in how to ensure information security while implementing cloud computing services.

**GSA Has Established Program Office and Cloud Computing Storefront, but Key Procurement Has Been Delayed in Part Due to Information Security Concerns**

GSA has established a Cloud Computing Program Management Office that manages several cloud computing activities within GSA and provides administrative support for cloud computing efforts by the federal Chief Information Officers (CIO) Council. Specifically, the program office manages a storefront, [www.apps.gov](http://www.apps.gov), established by GSA to provide a central location for federal agencies to purchase several software as a service cloud computing applications, including

- 
- business applications, such as data analysis, human resources, and financial management software, and tools for tracking and monitoring various types of activities;
  - office productivity applications, which include standard word processing and spreadsheet applications, and also applications used for brainstorming, collaboration, document management, and project management; and
  - social media applications that are focused on making it easier to create and distribute content and that enable people to communicate easily and share information.

GSA plans to expand the storefront by also providing infrastructure as a service cloud computing offerings such as storage, virtual machines, and Web hosting. To this end, GSA began a procurement process by issuing a request for quotations in July 2009. The request asked for quotations to provide the government with required documentation on vendors' offerings of cloud storage services, virtual machines, or cloud Web hosting. These services would be available through the [www.apps.gov](http://www.apps.gov) storefront. The procurement closed in September 2009, with nine vendors submitting quotations.

However, addressing information security issues has been a significant challenge in the procurement. GSA officials stated that as they were analyzing the submitted quotations, one issue they were attempting to resolve was establishing a process for federal agencies to work with GSA to complete the information security assessment and authorization process when using these services. In early March 2010, GSA canceled the request and announced plans to begin a new request process, in part due to concerns and challenges in addressing information security. Specifically, the new request will ask for services that meet the level of security for both low- and moderate-impact systems as defined in FIPS 199 and NIST SP 800-53. The canceled request required only low-level security. GSA stated that providing cloud computing services that meet both low- and moderate-impact information security controls would allow a broader range of services and customers. GSA officials also stated that they need to work with vendors after a new procurement has been completed to develop a shared assessment and authorization process, but have not yet developed specific plans to do so.

Adding moderate-impact controls to the request may increase demand for the infrastructure services when the procurement is completed; however, establishing both an assessment and authorization process for customers

---

Federal CIO Council Has Established Cloud Computing Executive Steering Committee but Has Not Finalized Key Process or Guidance

of these services and a clear division of security responsibilities will help ensure that these services, when purchased and effectively implemented, protect sensitive federal information.

The CIO Council established the Cloud Computing Executive Steering Committee to promote the use of cloud computing in the federal government. The GSA Cloud Computing Program Management Office provides technical and administrative support for the committee. The committee consists of an overall advisory council and these four subgroups:

- The communications subgroup provides information on the status of cloud computing in the federal government and is planning an information portal for the [www.apps.gov](http://www.apps.gov) storefront.
- The operational excellence subgroup examines cloud computing implementations at federal agencies, assists agencies in evaluating potential applications for cloud computing, and identifies possible improvements to the storefront.
- The standards subgroup is helping develop standards related to interoperability and portability of cloud computing services.
- The security subgroup is addressing several issues related to information security and cloud computing.

The security subgroup has begun developing recommendations for a streamlined assessment and authorization process through the Federal Risk and Authorization Management Program. This process would address authorizing operation of a system, including the development and implementation of risk assessments and security controls. For example, according to GSA, the program is to provide joint authorizations and continuous monitoring services for all federal agencies with an initial focus on cloud computing. The process would rely on several key steps of the process being performed by a governmentwide organization, while the final authorization to operate a system would still be made by a designated official at the agency purchasing the service. According to a summary provided by GSA, the goals for this process include providing better security and privacy, clearer communication of security requirements for government and industry, improved efficiency and broad acceptance for agencies, and compliance with existing federal information security guidance and legislation. Officials involved in the process have noted the

---

need to clearly delineate security control responsibilities between providers and customers. The group is currently working with its members to define interagency security requirements for cloud systems and services and related information security controls from both the moderate and low baselines specified in NIST SP 800-53 Revision 3.

According to GSA, a draft of the new assessment and authorization process has been approved by the Cloud Computing Executive Steering Committee. However, a deadline for completing development and implementation of this process had not been established. A particular concern of the committee is the requirement for agency CIOs to certify the adequacy of information security controls for systems that they do not own or operate. GSA officials involved in this effort stated that it may be up to OMB to clearly establish that agencies will be able to rely on the shared process.

In addition to the Executive Steering Committee and its subgroups, another component of the CIO Council is working on information security issues related to cloud computing. The group, which is part of the CIO Council's Information Security and Identity Management Committee, is currently developing a white paper on guidelines for the secure use of cloud computing for federal departments and agencies, according to a co-chair of this group. The paper is intended to provide agencies with guidelines, use cases, and scenarios to help program managers make risk-based decisions when selecting cloud deployment and service models.

Federal agencies responding to our information request, officials of the cloud computing case studies described in appendix II, and private sector representatives have all identified concerns with how to properly and efficiently complete activities related to the assessment and authorization process, including control selection and testing, when using cloud computing. Until a clear, comprehensive, and efficient process has been established, adoption of cloud computing in the federal government may be limited, and cloud computing programs that are implemented may not have appropriate information security controls in place.

**NIST Is Coordinating Activities with CIO Council but Has Not Established Cloud-Specific Guidance**

NIST is responsible for establishing information security guidance for federal agencies to support FISMA. Cloud computing is an emerging model for IT, and NIST has not yet established guidance specific to cloud computing. However, according to its officials, the institute has begun several other activities related to cloud computing. For example, it has developed a definition of cloud computing and is participating in the activities of the CIO Council subgroups.

---

The NIST official leading the institute's cloud computing activities stated that existing NIST requirements apply to cloud computing and can be tailored to the information security issues specific to cloud computing. However, as previously discussed in this report, both federal and private sector officials have made clear that existing guidance is not sufficient. At the conclusion of our review, NIST officials stated that the institute is planning to issue guidance on cloud computing and virtualization but had not yet finalized the topics that it would cover and had not determined a date for issuing this guidance.

Our analysis also indicates areas where existing NIST guidance does not clearly address information security issues specifically related to cloud computing. While NIST SP 800-53 covers general security areas important to cloud computing to some extent, the guidance lacks specificity in key security areas. For example, NIST guidance does not directly address key cloud computing security issues such as portability and interoperability, data center operations, and virtualization. Both public and private sector officials identified interoperability issues and concerns about virtualization as challenges agencies face when making decisions on whether to implement cloud computing. At the end of our review, NIST officials stated that SP 800-53 was not intended to be specific to a particular type of computing, such as cloud computing, but agreed that areas such as portability and interoperability were important in implementing cloud computing and they were considering including them in future NIST publications.

Furthermore, federal agencies stated that establishing a clear delineation of security control responsibilities between providers and customers is a challenge, but existing NIST guidance does not fully address these issues or establish a process for doing so. Existing NIST guidance addresses the establishment of interconnection security agreements between different organizations; however, the guidance is not specific to issues related to cloud computing. For example, NIST guidance does not address the division of information security responsibilities when several organizations are involved in cloud computing or possible variations in these roles and responsibilities due to the use of different cloud deployment and service models. Until federal guidance addresses information security issues specific to cloud computing and provides information on how to divide responsibilities between providers and customers, agencies may not be able to effectively ensure the security of their systems when using cloud computing.



---

## Conclusions

About half of the 24 agencies are using various models of cloud computing, and many others are interested in using it; however, implementation of this emerging technology presents both information security benefits and risks. Agencies have taken steps to address cloud computing security but have not always developed corresponding guidance. The use of attestation standards and precertification of cloud service providers may provide a way for agencies to ensure information security when using cloud computing service providers. However, OMB has not yet developed a strategy that addresses the information security issues related to cloud computing, and guidance from individual agencies and NIST to ensure information security is insufficient. While the federal CIO Council is developing a shared assessment and authorization process, which could help foster adoption of cloud computing, this process remains incomplete, and GSA has yet to complete its procurement of cloud computing infrastructure as a service offerings for its storefront, in part due to security concerns. Until federal guidance and processes that specifically address information security for cloud computing are developed, agencies may be hesitant to implement cloud computing, and those programs that have been implemented may not have effective information security controls in place.

---

## Recommendations for Executive Action

To assist federal agencies in identifying uses for cloud computing and information security measures to use in implementing cloud computing, we recommend that the Director of OMB take the following three actions:

- Establish milestones for completing a strategy for implementing the federal cloud computing initiative.
- Ensure the strategy addresses the information security challenges associated with cloud computing, such as needed agency-specific guidance, the appropriate use of attestation standards for control assessments of cloud computing service providers, division of information security responsibilities between customer and provider, the shared assessment and authorization process, and the possibility for precertification of cloud computing service providers.
- Direct the CIO Council Cloud Computing Executive Steering Committee to develop a plan, including milestones, for completing a governmentwide security assessment and authorization process for cloud services.

To assist federal agencies in selecting and acquiring precertified cloud computing products and services, we recommend that the Administrator

---

of GSA, as part of the procurement for infrastructure as a service cloud computing technologies, ensure that full consideration is given to the information security challenges of cloud computing, including a need for a shared assessment and authorization process.

To assist federal agencies in implementing appropriate information security controls when using cloud computing, we recommend that the Secretary of Commerce direct the Administrator of NIST to issue cloud computing information security guidance to federal agencies to more fully address key cloud computing domain areas that are lacking in SP 800-53, such as virtualization, data center operations, and portability and interoperability, and include a process for defining roles and responsibilities of cloud computing service providers and customers.

---

## Agency Comments and Our Evaluation

In providing comments on a draft of this report, OMB, GSA, and the Department of Commerce, stated that they generally concurred with the contents and recommendations of the report. The agencies' comments and our responses are summarized below:

- In written comments on a draft of this report, the Federal Chief Information Officer stated that OMB agreed with our recommendations. He described efforts under way for developing a cloud computing strategy, stating that OMB intends to develop such a strategy over the next 6 months. In addition, he stated that OMB agrees that the strategy must address the security challenges associated with implementing cloud computing and has established a group to study, propose, and implement a solution for governmentwide assessment and authorization. The Office of Management and Budget's comments are reprinted in appendix III.
- In written comments on a draft of this report, the Administrator of GSA stated that GSA agreed in part with our findings and recommendation to complete the procurement for infrastructure as a service cloud computing technologies and ensure that it includes full consideration of the information security challenges of cloud computing. The Administrator stated that GSA will reissue the procurement request in May 2010. She also provided additional information on the Federal Risk and Authorization Management Program, which we have incorporated in the report as appropriate. In subsequent discussions with GSA, we revised our recommendation to clarify its intent, and agency officials stated that GSA had reissued the request on May 12, 2010, and fully agreed with our recommendation. GSA's comments are reprinted in appendix IV.

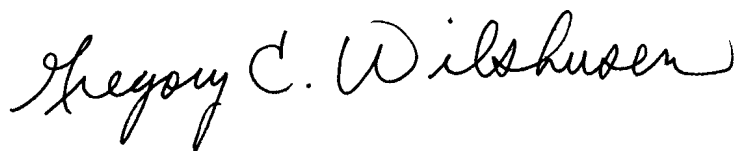
- 
- In written comments on a draft of this report, the Secretary of Commerce concurred with our recommendation. He noted that NIST expects to release a virtualization document for public comment in June 2010 and release a cloud computing document for public comment in September 2010. In addition, the Secretary provided technical comments which we incorporated in the draft as appropriate. Comments from the Department of Commerce are reprinted in appendix V.

We provided a draft of this report to the other 22 major federal agencies to which we did not make recommendations and received technical comments from 4 agencies. We have incorporated these comments in the report as appropriate.

---

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to interested congressional committees, the Director of OMB, the Secretary of Commerce, and the Administrator of GSA. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staffs have any questions about this report, please contact me at (202) 512-6244 or at [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix VI.



Gregory C. Wilshusen  
Director, Information Security Issues

---

*List of Congressional Requesters*

The Honorable Joseph I. Lieberman  
Chairman

The Honorable Susan M. Collins  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Tom R. Carper  
Chairman  
Subcommittee on Federal Financial Management, Government  
Information, Federal Services, and International Security  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Diane E. Watson  
Chairwoman  
Subcommittee on Government Management, Organization,  
and Procurement  
Committee on Oversight and Government Reform  
House of Representatives

---

# Appendix I: Objectives, Scope, and Methodology

---

The objectives of our review were to (1) identify the models of cloud computing; (2) identify the information security implications of using cloud computing services in the federal government; and (3) assess federal guidance and efforts to address information security when using cloud computing.

To identify cloud computing models, we reviewed publications, white papers, and other documentation from public and private sector organizations. We then obtained relevant information through interviews with officials from the National Institute of Standards and Technology (NIST) and private sector organizations that offer cloud computing services. We compared cloud computing descriptions and definitions of cloud computing from these sources to identify similarities and differences.

To identify the information security implications of using cloud computing services in the federal government, we reviewed documentation from the public and private sectors. Our documentation review focused on identifying the positive and negative information security implications (risks and benefits) of cloud computing. We supplemented this review by interviewing representatives of public and private sector organizations to prioritize these implications and identify information security challenges associated with federal agencies working with cloud computing service providers. We interviewed representatives of several of the 24 major federal agencies<sup>1</sup> and private sector organizations that provide cloud computing services. In addition, we issued a survey and data request to the 24 federal agencies. We pretested the survey at three agencies to ensure that the questions were relevant and easy to comprehend. For each agency surveyed, we identified the appropriate point of contact, notified each one of our work, and distributed the survey along with a data request to each via e-mail in November 2009. All 24 agencies responded to our survey and data request from December 2009 to February 2010; results are reported as of this date. We contacted agency officials when necessary for additional information or clarification of agency responses. We did not verify the

---

<sup>1</sup>The 24 agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to corroborate information provided in their responses. We then analyzed the results of the survey and data request responses to identify

- the potential information security implications agencies might consider positive or negative for cloud computing;
- the techniques agencies are using to ensure that effective information security measures are being implemented when using cloud computing;
- the extent to which the agency has procured or plans to procure cloud computing products or services using [www.apps.gov](http://www.apps.gov); and
- the concerns agencies faced when working with cloud computing providers.

Conducting any survey may introduce errors. For example, differences in how a particular question is interpreted, the sources of information that are available to respondents, or how the data are entered or were analyzed can introduce variability into the survey results. We took steps in the development of the survey instrument, the data collection, and the data analysis to minimize errors.

To assess federal guidance and efforts to address information security when using cloud computing, we gathered and analyzed information at federal entities with specific governmentwide responsibilities, including the Office of Management and Budget (OMB), General Services Administration (GSA), NIST, and the federal Chief Information Officers Council. We further reviewed federal information security guidance to determine the extent to which the guidance addressed concerns specifically related to cloud computing and relevant information security areas. For example, we compared NIST Special Publication 800-53 Revision 3 to key cloud computing security areas specified by other IT security organizations such as the Cloud Security Alliance and European Network and Information Security Agency. We also conducted case studies on three federal cloud computing programs, the Department of Defense's (DOD) Rapid Access Computing Environment (RACE) program, the National Aeronautics and Space Administration's (NASA) Nebula program, and the Department of Transportation's (DOT) Car Allowance Rebate System (CARS) program. We selected these agency case studies based on cloud computing experts' and agency officials' referrals, and any references in the documentation we reviewed. We also relied on the

survey of the 24 major federal agencies to identify the techniques federal agencies stated they used to ensure that effective information security measures are in place when they use cloud computing.

We conducted this performance audit from September 2009 through May 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

# Appendix II: Cloud Computing Case Studies

---

## DOD's RACE Program Provides Platforms for DOD Systems Development Efforts

The following is a description of three federal cloud computing programs: the DOD's RACE program; NASA's Nebula program; and Department of Transportation's CARS program, including lessons learned related to information security.

The RACE program was started by DOD's Defense Information Systems Agency in October 2008 to provide platform as a service to support DOD systems development efforts. The goal of the program is to provide the service through a streamlined process including system provisioning, development, testing, assessment and authorization, and deployment of applications to DOD customers within a private cloud. RACE customers purchase one or many virtual machines<sup>1</sup> through a self-service portal. The RACE program is managed by both government and contractor personnel within existing DOD data centers and operates only on DOD's internal network.

According to program officials, users can acquire server capacity rapidly for short- or long-term use without the need for approval for a capital acquisition expense. Initial provisioning in RACE takes a few days, while traditional purchasing can take a month or longer. RACE currently has about 120 virtual machines in use. Program officials state that they hope to expand RACE to the classified environment in the future. Currently, DOD uses three information system impact levels,<sup>2</sup> which are equivalent to low, moderate, and high, as defined by NIST. RACE is currently certified to operate at the moderate-impact level, although the current use is for data at the lowest impact level.

### Information Security Controls and Lessons Learned

DOD officials emphasized the need for a clear division of responsibilities among its customers and cloud service providers when implementing cloud computing. For RACE, potential customers must agree to meet minimum information security requirements before becoming customers

---

<sup>1</sup>A virtual machine is a software image of a computer that executes programs in the same manner as a physical computer or server. Multiple virtual machine images can run on one physical computer.

<sup>2</sup>DOD categorizes system impact levels using Mission Assurance Category I, II, and III: category I systems are considered high impact and handle information that is vital to mission success, category II systems are considered medium impact and handle information that is important for mission success, and category III systems are considered low impact and handle information that does not materially affect mission success.



---

of the RACE program, including resolving any open vulnerabilities or documenting them in a plan of action and milestones. The program also has documentation that divides information security control responsibilities between controls managed by the RACE program and controls managed by the customer. Using a matrix containing the appropriate DOD information assurance controls, RACE officials determined that out of 106 controls, 62 were the responsibility of the customer, 31 of the service provider, and 13 were not applicable. Of the 106 controls, 37 were classified as inheritable controls, meaning the customer application inherits several predefined information assurance controls from RACE.

During the initial stages of RACE implementation, program officials recognized the need to improve related DOD business processes, including those related to security. The existing DOD process required for risk assessment and assessment and authorization for information systems created challenges because of its focus on stand-alone systems and multiple levels of organizational review. In response, the program office worked with a contractor to re-engineer the process to complete information security requirements for new systems. Program officials estimate that the total time required to complete the assessment and authorization process will be reduced from 80 days to 40 days for RACE customers, but the process is too new to be verified. A subsequent release is planned to further reduce this time to 7 days. The officials stated that overall implementation of the RACE program and other cloud efforts would have been faster if guidance and processes related to assessment and authorization for cloud computing had already been in place.

#### NASA's Nebula Pilot Uses Open-Source Technologies to Enhance Collaboration

Nebula is a cloud computing pilot under development at NASA's Ames Research Center in Mountain View, California. It is an infrastructure as a service implementation for scientific data and Web-based applications. Platform as a service capability is planned for the future. According to NASA, Nebula is to provide high-capacity computing, storage, and network connectivity using a virtualized, scalable approach to achieve cost and energy savings. Currently, NASA's Nebula is considered a private cloud and is operated at Ames Research Center on NASA equipment using both government and contractor personnel. Nebula is housed in a standard shipping container that is mounted in place, but could be transported if needed (see fig. 4). Program officials chose this design as a means to easily replicate the Nebula equipment as the program expands. The officials state that a future goal is for Nebula to become a hybrid cloud as a way to eventually foster collaboration in analysis of NASA-sponsored research with the academic community and the public. As a result, Nebula relies on

open-source cloud computing technologies so that data can be easily transferred to other cloud service providers if required. The officials stated that when NASA data is first generated, its sensitivity must be evaluated to see if it is appropriate for public release. Once the decision has been made to share the data, the use of Nebula makes sharing information easier.

The officials also stated that Nebula will provide other benefits. For example, according to NASA, researchers who use Nebula will not have to purchase their own servers, hardware, and computing infrastructure, which can be time-consuming. Nebula is currently authorized to handle only low-impact data as defined in FIPS 199; however, officials noted that they may migrate to a moderate-impact system in the future. Currently, Nebula's customers include the World Wide Telescope from Ames Research Center and the Climate Grid led by NASA's Goddard Space Flight Center.

---

**Figure 4: NASA Nebula Container**



Source: NASA.

### **Information Security Controls and Lessons Learned**

NASA officials said that a major challenge in their implementation of Nebula was determining how to apply federal information security policies

---

and guidance because current federal guidance does not clearly address specific controls for a cloud computing environment like Nebula. Examples included how to track, schedule, and report compliance with the Federal Information Security Management Act of 2002 when customers are responsible for some controls and the provider is responsible for others, and how to address security and service-level agreements. Nebula officials noted challenges in determining responsibilities and identifying the necessary documentation for interconnection security agreements<sup>3</sup> between customers and third-party systems used by the customers.

Additionally, officials noted the need to clearly define the information security controls for which the cloud provider is responsible and those for which the customer is responsible. For example, effective incident response in a cloud environment requires delineation of customer and provider responsibilities, which is information that is not currently addressed in federal guidance. NASA Nebula officials noted that the exact number of controls for which the customer is responsible varies depending on the cloud computing service model. In Nebula's current infrastructure as a service offering, the customer is responsible for 47 of the 112 total controls in NIST SP 800-53 Revision 3 for low-impact systems. They noted further that many of the responsibilities under the customer controls are actually shared between the customer and Nebula, as the service provider, because the provider will still have responsibility for the parts of the infrastructure under the provider's control.

#### DOT's CARS Program Made Partial Use of Cloud Computing, but Was Limited by Security Concerns

The CARS program used a public cloud for part of its system. CARS was administered by DOT under the authority of the Consumer Assistance to Recycle and Save Act of 2009. The program allowed owners of certain less fuel-efficient vehicles to receive a credit for trading in a vehicle and purchasing or leasing a new, more fuel-efficient vehicle. Dealers were reimbursed for this credit by the government. According to program officials, the program faced a number of challenges, including having only about 1 month to develop and deploy the system and an unexpectedly high demand for the program; users of the program tripled in number within 12 days of the start of the program.

---

<sup>3</sup>An interconnection security agreement documents security roles and responsibilities and technical requirements related to the connection of two information systems.

The program, which operated from July 24 to August 24, 2009, had two major information technology components: a publicly accessible Web site with content for consumers, dealers, and salvage facilities, and a payment processing system used by dealers to submit applications to the program. The Web site was considered a low-impact system under FIPS 199, but the payment processing system, which contained personal information, was considered a moderate-impact system.

The public Web site used a cloud computing service provider that hosted the Web site and provided additional surge capabilities to cope with spikes in demand for Web content. Effective communication through the Web site was vital to implementation of the CARS program. According to department officials, because of the use of a cloud service provider, the CARS Web site was not affected by the July 4, 2009, cyber attacks.<sup>4</sup> Also, using the cloud service provider for Web content allowed the CARS program information to be accessible while protecting DOT's primary Web site from being overwhelmed and potentially disabled by the high demand for information about the program. The department's agreement with the cloud service provider allowed it to quickly and easily increase capacity as needed.

In contrast, the payment-processing system used a more traditional database and financial management system containing commercial off-the-shelf software and, according to DOT officials, was not able to cope with increases in demand for the program. Although the payment processing system was originally designed to process up to 250,000 transactions over 4 months, the system actually processed approximately 690,000 transactions in about 1 month. Partly as a result of the overwhelming interest in the program, the department encountered several technical issues and capacity-related deficiencies with the payment system. Specifically, the system had numerous outages and periods of slow operation, causing frustration among dealers and disrupting the department's ability to review submissions. Since the payment processing system did not use cloud computing, expanding the system's capacity was more challenging.

---

<sup>4</sup>In July 2009, press accounts reported that a widespread and coordinated attack over the course of several days had targeted Web sites operated by major government agencies, causing disruptions to the public availability of government information.

---

### Information Security Controls and Lessons Learned

Officials said they briefly considered use of a cloud computing model for the payment processing system, but were reluctant to do so because of programmatic constraints to using applications already in use by the department. They also were concerned about processing personal information in a cloud environment without the environment having been precertified to handle the information. The officials acknowledged that many characteristics of the CARS program would have made the payment processing system a good candidate for cloud computing. These included the program's limited time available for deployment, short duration, and need to cope with sudden peaks in demand. However, the need to interface with existing department computing infrastructure, including using expertise from the existing vendor and the lack of an already developed and deployed cloud that had been certified to handle personal information made them hesitant to use a cloud computing solution and led them to instead use a more traditional application. As it was, the short time available to deploy the system made completion of information security processes, such as authorization and accreditation, a challenge.

A program official added that successful implementation of cloud computing in the federal government will be dependent on several information security-related factors, including the ability to ensure continuous monitoring of security controls and the ability to independently verify the security of cloud computing providers.

# Appendix III: Comments from the Office of Management and Budget



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

Gregory Wilshusen  
Director  
The Government Accountability Office  
441 G Street, Northwest  
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on your draft report, "INFORMATION SECURITY: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing" (GAO-10-153).

As an initial matter, OMB appreciates GAO's focus on this important issue, and we agree with GAO on the need for an overarching Federal cloud computing strategy with milestones. However, cloud computing is in its early stages. OMB has been deliberate in making sure a unified cloud strategy does not thwart innovation by prematurely hardwiring and institutionalizing cloud technologies, standards and security requirements. Accordingly, OMB, Federal agencies and private industry are partnering together to observe, test and deploy best practices as the cloud sector matures. OMB feels it would be appropriate to develop, over the next six months, a Federal cloud strategy that covers a planning horizon of five to 10 years and is based on lessons learned in the near term. Additionally, the strategy and related milestones may need to evolve over time, as cloud computing technologies establish market strongholds.

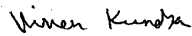
As noted above, we agree that the strategy must address the security challenges associated with implementing cloud computing. For this reason the National Institute of Standards and Technology (NIST), at the direction of the Federal CIO, is convening a cloud summit on May 20<sup>th</sup>, 2010. The Summit, which will feature a broad array of speakers from government, industry and academia, will broaden the dialogue on key cloud issues, including data interoperability, portability and security standards. Outputs from the Summit will be used to guide the development of appropriate security controls and inform a future Federal cloud computing strategic plan.

OMB is committed to the Federal government developing and implementing secure cloud environments, and we are actively working to make this a reality. To that end, the Federal CIO has established the Cloud Computer Security Workgroup (led by NIST) to study, propose and implement a solution for government-wide security assessment and authorization. This Workgroup has already established a process for government-wide assessments and authorizations.

Moreover, agency-specific guidance must address standards and the appropriate division of roles and responsibilities. The Federal CIO has also activated a standards workgroup, and OMB is working with NIST to propose and implement standards for implementing cloud computing environments in support of government programs and activities. Agencies recognize the need for agency-specific guidance in this area, and they are collaborating with OMB to align our cloud computing initiatives with agency business needs.

Thank you again for the opportunity to comment on the draft report and to discuss our work on the development and implementation of a secure cloud computing environment.

Sincerely,



Vivek Kundra  
Federal Chief Information Officer

# Appendix IV: Comments from the General Services Administration



GSA Administrator

May 7, 2010

The Honorable Gene L. Dodaro  
Acting Comptroller General of the United States  
U.S. Government Accountability Office  
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the draft report entitled "Federal Guidance needed to Address Control Issues with Implementing Cloud Computing" (GAO-10-513).

We agree in part to the findings and recommendations. Substantive comments to the findings and recommendations are provided below:

1. **The report recommends that "the CIO Council Cloud Computing Executive Steering Committee develop a plan, including milestones, for completing a government wide security assessment and authorization process for cloud services.**

The Security Working Group has developed the Federal Risk and Authorization Management Program (FedRAMP) that addresses this recommendation. The Security Working Group, as part of GSA's Cloud Computing Program with members from over 15 agencies, is led by the National Institute of Standards and Technology (NIST). FedRAMP is a government-wide program to provide joint authorizations and continuous security monitoring services for all Federal agencies with an initial focus on cloud computing. It is a major element in the strategy to facilitate the use of cloud computing by the Federal Government. FedRAMP is a central office that performs certification and authentications, recommends authority to operate, and supports continuous monitoring of systems in compliance with Federal laws and regulations. Agencies can leverage the Certification and Authorization (C&A) and Authority to Operate (ATO) without having to repeat the process for each system. We expect that FedRAMP will be operational in May 2010.

As detailed in the GAO Report, agencies have expressed the following concerns: (a) depending on vendors ability to provide and maintain adequate security controls; (b) implementing and maintaining adequate security controls and monitoring; and (c) meeting the requirements of Federal information security requirements and guidance. Each agency is responsible to independently select appropriate security controls, implement and assess security, develop appropriate plans of action, and conduct ongoing security monitoring.

U.S. General Services Administration  
1800 F Street, NW  
Washington, DC 20405-0002  
Telephone: (202) 501-0800  
Fax: (202) 219-1243  
www.gsa.gov



2

As background, FedRAMP is a unified government-wide risk management for enterprise level IT systems. It enables agencies to leverage authorizations with:

- Unified interagency C&A process;
- Consistent application of Federal security requirements;
- Consolidated risk management; and
- Increased effectiveness and management cost savings.

FedRAMP has three components:

- Security Requirement Authorities to create governmentwide baseline security requirements that are interagency developed and approved;
- FedRAMP Office to coordinate authorization packages, manage authorized system list, and provide continuous monitoring oversight; and
- Joint Authorization Board to perform authorizations and on-going risk determinations that can be leveraged government-wide. Members of the Board are GSA, DoD, DHS and the sponsoring agency for the system to be authorized.

Figure 1 presents a concept of operations and high level workflow for FedRAMP.

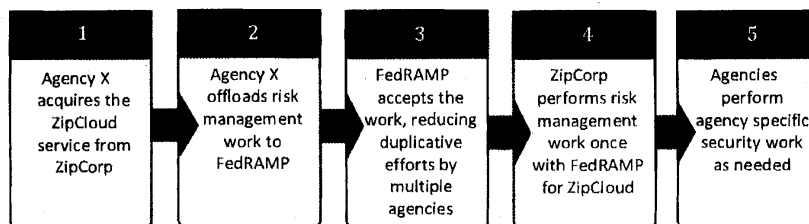


Figure 1. FedRAMP Workflow

FedRAMP will create a unified risk management process that:

- **increases security** through focus assessments;
- **eliminates duplication of effort** and associated cost savings;
- **enables rapid acquisition** by leveraging pre-authorized solutions;
- provides agency vetted **transparent security** requirements and authorization packages;
- facilitates **multi-agency use** of shared systems; and
- ensures **integration with governmentwide security** efforts.

3

FedRAMP allows agencies to leverage authorizations which reduces agency effort for authorizations and monitoring. With FedRAMP agencies will only have to review security details, leverage the existing authorization, and secure agency usage of system. This will greatly reduce cost, enable rapid acquisition, and reduce effort (diagrams that illustrate FedRAMP processes are enclosed).

Currently, it is anticipated that FedRAMP will be operational in May 2010.

2. **The GAO report recommends that “the Administrator of GSA complete the procurement for pre-certified infrastructure as a service cloud computing technologies at the low and moderate impact levels and ensure that it includes full considerations of the information security challenges of cloud computing, including a need for a shared assessment and authorization process.”**

GSA will reissue the Request for Quote for Infrastructure as a Service (IaaS) in May 2010. The RFQ will result in a multi-award blanket purchase agreement (BPA) for IaaS providers. Awardees of this BPA will be included in FedRAMP. FedRAMP is a government-wide program to provide joint authorizations and continuous security monitoring services for all Federal agencies with an initial focus on cloud computing. Upon successful completion of the FedRAMP process and approval by the Joint Approval Board, the IaaS services will be granted an Authority to Operate (ATO) at the moderate impact level as defined by the Federal Information Security Management Act. An ATO at the moderate level includes approval of operation at low impact level.

Before reissuing the RFQ, GSA is working to improve the statement of work and to clarify the bidding instructions. As a result, the RFQ will better reflect customer requirements and vendors will be able to more accurately bid their services against requirements.

If you have any additional questions or concerns, please do not hesitate to contact me. Staff inquiries may be directed to Ms. Katie Lewin, Director, Cloud Computing Program, Office of Citizen Services and Communications. She can be reached at (202) 219-0394.

Sincerely,

  
Martha Johnson  
Administrator

Enclosure

cc: Gregory C. Wilshusen

# Appendix V: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE  
The Secretary of Commerce  
Washington, D.C. 20230

May 4, 2010

Mr. Gregory C. Wilshusen  
Director, Information Security Issues  
United States Government Accountability Office  
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report from the Government Accountability Office (GAO) entitled "Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing" (GAO-10-513).

We concur with the report's conclusions that Federal agencies should take several steps to address cloud computing security, including completing the strategy, considering security in a planned procurement of cloud computing services, and issuing guidance related to cloud computing security. The Department of Commerce offers the following comments regarding the GAO's conclusions:

1. Page 14. The draft states that "Infrastructure as a service is the foundation of all cloud services." This is not accurate because one can build cloud services without relying on an "infrastructure as a service" system. We suggest deleting the sentence.
2. Page 24. The NIST point about browser vulnerability (from page 23) should be part of table 3.
3. Page 24. Delete "and it does not currently have finalized plans or milestones to issue cloud-specific security guidance" and replace it with "NIST has two documents in preparation: a guide on virtualization and a guide on cloud computing. NIST expects the virtualization document to be released for public comment in June 2010 and the cloud computing document to be released for public comment in September 2010."
4. Page 32. Replace "stated that existing NIST guidance applies" with "stated that existing NIST requirements apply."

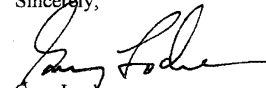
Note: NIST publication 800-53 is a catalogue of controls that represent security requirements for information systems. It is designed to be flexible and adaptable to a variety of computing models and technologies, including cloud computing. We agree that guidance specific to cloud computing is needed.

Mr. Gregory C. Wilshusen  
Page 2

5. Page 33. NIST believes portability and interoperability are not "security issues," as the text implies in the second paragraph on the page. We suggest replacing the sentence "For example, NIST guidance does not clearly address key cloud computing security issues such as portability and interoperability, data center operations, and virtualization" with "Current NIST guidance does not directly address key cloud computing issues such as portability and interoperability, data center operations, and virtualization."

We welcome further communications with GAO regarding its conclusions and look forward to receiving the final report. Please contact Rachel Kinney at (301) 975-8707 if you have any questions regarding this response.

Sincerely,



Gary Locke

---

# Appendix VI: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov)

---

## Staff Acknowledgments

In addition to the contact name above, individuals making contributions to this report included Vijay D'Souza (Assistant Director), Season Dietrich, Neil Doherty, Nancy Glover, Dana Pon, Jason Porter, and Shaunyce Wallace.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

